Базовый интерфейс защиты DOCSIS 1.0 в Cisco CMTS

Содержание

Введение

Основная цель Базового интерфейса обеспечения конфиденциальности (BPI) DOCSIS должна предоставить схему шифрования простых данных для защиты данных, передаваемых и от кабельных модемов в Данных по Кабельной сети. Базовые средства защиты сети связи от несанкционированного доступа можно использовать для аутентификации кабельных модемов и для авторизации передачи группового трафика кабельным модемам.

Система Cisco Cable Modem Termination System (CMTS) (CMTS) и продукты кабельного модема рабочие образы программного обеспечения Cisco IOS с набором функций включая символы "k1" или "k8" поддерживает Базовую конфиденциальность, например ubr7200-k1p-mz.121-6. EC1.bin.

Этот документ обсуждает Базовую конфиденциальность на продуктах Cisco, работающих в режиме DOCSIS1.0.

Перед началом работы

Условные обозначения

Дополнительные сведения об условных обозначениях см. в документе Технические рекомендации Cisco. Условные обозначения.

Предварительные условия

Для данного документа отсутствуют предварительные условия.

Используемые компоненты

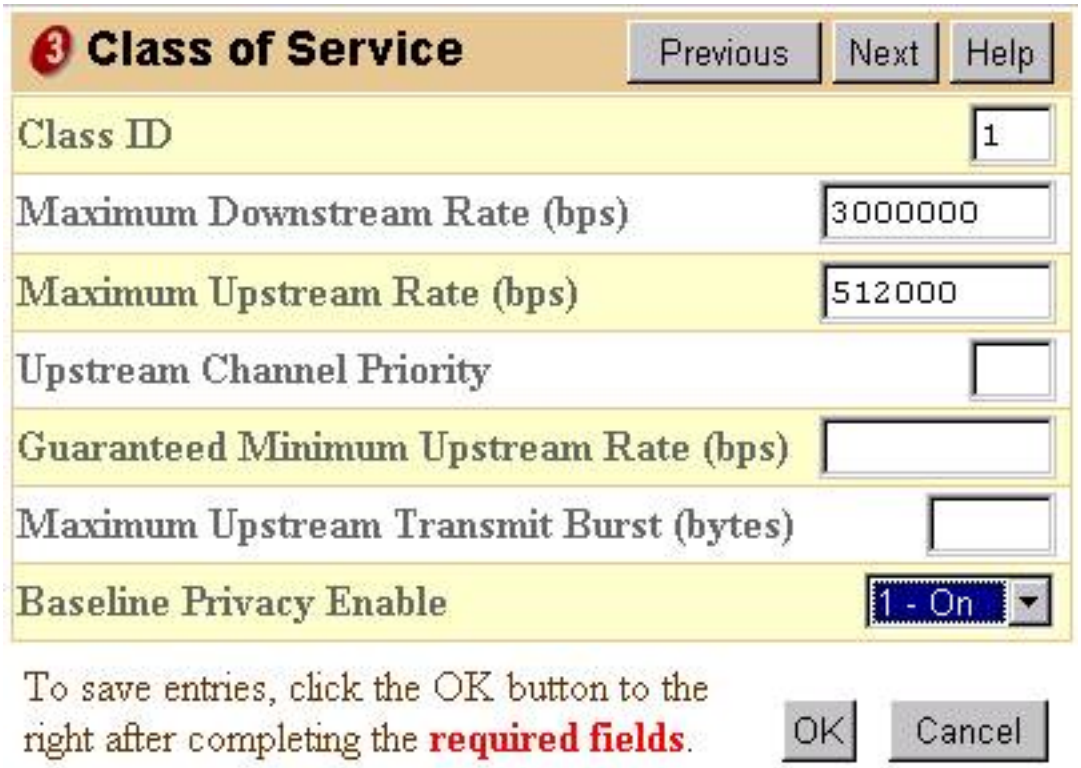
Сведения в этом документе основываются на настройке uBR7246VXR рабочий релиз 12.1 программного обеспечения Cisco IOS (6) EC, но это также применяется ко всем другим Продуктам CMTS Cisco и выпускам ПО.

Сведения, содержащиеся в данном документе, были получены с устройств в специальной лабораторной среде. Все устройства, описанные в данном документе, были запущены с конфигурацией по умолчанию. При работе с реальной сетью необходимо полностью осознавать возможные результаты использования всех команд.

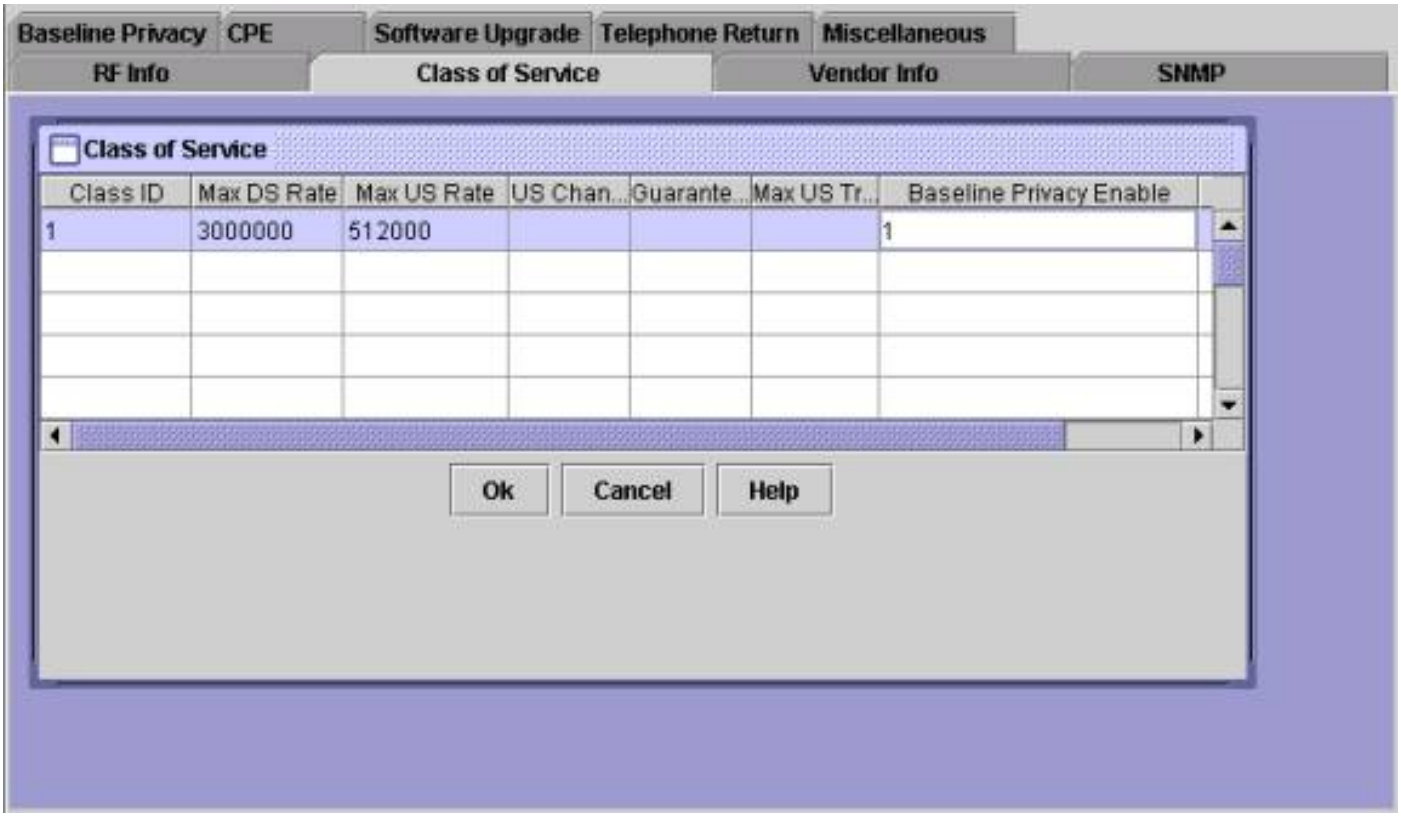
Настройка базовой безопасности для кабельных модемов

Кабельный модем только попытается использовать Базовую конфиденциальность, если этим дадут команду сделать так через параметры Класса обслуживания в файле конфигурации DOCSIS. Файл конфигурации DOCSIS содержит рабочие параметры для модема и загружен через TFTP как часть процесса того, чтобы подключаться к сети.

Один метод создания файла конфигурации DOCSIS должен использовать Конфигуратор Кабельного модема DOCSIS на Cisco.com. Использование Конфигуратора Кабельного модема DOCSIS, можно создать файл конфигурации DOCSIS, который дает команду, чтобы Кабельный модем использовал Базовую конфиденциальность путем установки поля Enable Конфиденциальности Базовой конфиденциальности под вкладкой Class of Service к **На**. См. пример ниже:



Также автономная версия конфигурации файла DOCSIS от может использоваться для включения Базовой конфиденциальности как показано ниже:



Как только создан файл конфигурации DOCSIS с поддержкой BPI, нужно сбросить кабельные модемы, чтобы загрузить новый файл конфигурации и впоследствии использовать базовую конфиденциальность.

Проверка кабельного модема на использование базовой конфиденциальности

При использовании Cisco CMTS с помощью команды "show cable modem" можно просмотреть состояние каждого из кабельных модемов. Существует несколько возможных состояний модема, использующего базовую конфиденциальность.

онлайн

После того, как кабельный модем регистрируется в CMTS Cisco, он вводит онлайновое состояние. Кабельный модем должен добраться до этого состояния, прежде чем это сможет выполнить согласование о параметрах Базовой конфиденциальности с CMTS Cisco. На этом этапе трафик данных, передаваемый между кабельным модемом и CMTS, дешифрован. Если кабельный модем остается в том же состоянии и не переходит в указанные ниже режимы, то он не выполняет базовую конфиденциальность.

онлайновый (pk)

Онлайновое (pk), состояние означает, что Кабельный модем был в состоянии выполнить согласование **о Ключе авторизации**, иначе известном как **Ключ шифрования (KEK)** с CMTS Cisco. Это означает, что кабельному модему разрешено использовать базовую конфиденциальность, и он успешно согласовал первую фазу базовой конфиденциальности. KEK является ключом на 56 битов, используемым для защиты последующих согласований базовой конфиденциальности. Когда модем находится в онлайновом (pk), трафик данных состояния, передаваемый между кабельным модемом и CMTS Cisco, все еще дешифрован, поскольку ни о каком ключе для трафика шифрования данных еще не выполнили согласование. Как правило, онлайновый (pk) придерживается онлайновым (pt).

отклонение (pk)

Это состояние указывает, что попытки кабельного модема согласования с KEK были неудачными. Наиболее распространенная причина, что модем был бы в этом состоянии, будет состоять в том, что CMTS Cisco включили аутентификацию модема, и модем имеет ошибку проверки подлинности.

online (pt)

На этом этапе модем успешно выполнил согласование о Ключе шифрования трафика (TEK) с CMTS Cisco. TEK используется для шифрования трафика данных между CMTS Cisco и Кабельным модемом. Процесс согласования TEK шифруется с помощью KEK. TEK является ключом на 56 или 40 битов, используемым для шифрования трафика данных между CMTS Cisco и кабельным модемом. На этом этапе базовая конфиденциальность успешно установлена и выполнение, поэтому пользовательские данные, передаваемые между CMTS Cisco и кабельным модемом, шифруются.

отклонение (pt)

Это состояние указывает, что кабельный модем был неспособен успешно выполнить согласование о TEK с CMTS Cisco.

Ниже см. пример результата команды show cable modem, показывающие кабельные модемы в различных состояниях, относящиеся к базовой конфиденциальности.

```
CMTS# show cable modem
Interface    Prim Online      Timing Rec    QoS CPE IP address      MAC address
             Sid  State       Offset Power
Cable3/0/U1 1    online(pt)  2208    0.75  7   0   10.1.1.40       0020.4001.5370
Cable3/0/U1 2    online(pk)  2213    0.50  5   0   10.1.1.33       0050.7366.1fb9
Cable3/0/U0 3    online(pt)  2738    0.00  5   0   10.1.1.24       0002.fdfa.0a35
Cable3/0/U1 4    reject(pk)  2738    1.00  5   0   10.1.1.30       0001.9659.4447
```

Примечание: Более подробно данные по статусу кабельного модема представлены в разделе "Устранение неисправностей кабельных модемов uBR без выхода в сеть".

Таймеры, влияющие на установление и техническое обслуживание базовой конфиденциальности

Существуют определенные значения времени ожидания, которые могут корректироваться для смены поведения базовой конфиденциальности. Некоторые из этих параметров могут быть настроены на CMTS Cisco и других через файл конфигурации DOCSIS. Существует мало причины изменить любой из этих параметров за исключением времени жизни KEK и срока действия TEK. Эти таймеры можно изменять с целью усиления безопасности кабельной системы или сокращения затрат ресурсов CPU и дополнительных объемов трафика, связанных с управлением BPI.

Время жизни KEK

Время жизни KEK является периодом времени, что Кабельный модем и CMTS Cisco должны полагать, что согласованный KEK допустим. Прежде чем этот период времени прошел, кабельный модем должен пересмотреть новый KEK с CMTS Cisco.

Можно настроить на этот раз использование команды кабельного сопряжения CMTS Cisco:

cable privacy kek life-time *300-6048000 seconds*

Настройка по умолчанию 604800 секунд, что равняется семи дням.

При наличии меньшего повышения безопасности системы времени жизни KEK, потому что каждый KEK продлится более короткий период времени и следовательно если KEK будет взломан, меньше будущих согласований TEK было бы восприимчиво к тому, чтобы быть угнанным. Недостаток к этому - то, что пересмотр KEK увеличивает загрузку ЦПУ на трафике управления BPI кабельных модемов и увеличений на кабельном участке.

Льготное время KEK

Льготное время KEK является периодом времени, прежде чем время жизни KEK истечет, что кабельный модем предназначается, чтобы начать выполнять согласование с CMTS Cisco относительно нового KEK. Идея, стоящая за присутствием этого таймера, заключается в том, что у кабельного модема есть достаточно времени для обновления KEK до его истечения.

Можно настроить на этот раз использование команды кабельного сопряжения CMTS Cisco:

cable privacy kek grace-time *60-1800 seconds*

Это значение времени можно также настроить с помощью файла конфигурации DOCSIS, указав его в поле Authorization Grace Timeout на вкладке Baseline Privacy. Если это поле файла конфигурации DOCSIS заполнено в тогда, оно имеет приоритет по любому значению, настроенному на CMTS Cisco. Значение по умолчанию для этого таймера равно 600 секундам, что равно 10 минутам.

Срок действия TEK

Срок действия TEK является периодом времени, что Кабельный модем и CMTS Cisco должны полагать, что согласованный TEK допустим. Прежде чем этот период времени прошел, кабельный модем должен пересмотреть новый TEK с CMTS Cisco.

Можно настроить на этот раз использование команды кабельного сопряжения CMTS Cisco:

cable privacy tek life-time <180-604800 seconds>

По умолчанию установлено значение 43200 с (12 часов).

При наличии меньшего времени жизни TEK повышает уровень безопасности, потому что каждый TEK продлится более короткий период времени и следовательно если TEK будет взломан, меньше данных будет представлено неавторизованной расшифровке. Недостаток к этому - то, что пересмотр TEK увеличивает загрузку ЦПУ на трафике управления BPI кабельных модемов и увеличений на кабельном участке.

Подготовительный срок TEK

Льготное время TEK является периодом времени, прежде чем срок действия TEK истечет, о котором кабельный модем предназначается, чтобы начать выполнять согласование с CMTS Cisco для нового TEK. Идея позади наличия этого таймера состоит в том так, чтобы кабельный модем имел достаточно времени для возобновления TEK, прежде чем это истечет.

Можно настроить на этот раз использование команды кабельного сопряжения CMTS Cisco:

cable privacy tek grace-time *60-1800 seconds*

Можно также настроить это время с помощью файла конфигурации DOCSIS, заполнив поле TEK Grace Timeout на вкладке Baseline Privacy. Если это поле файла конфигурации DOCSIS заполнено в тогда, оно имеет приоритет по любому значению, настроенному на CMTS Cisco.

Значение по умолчанию для этого таймера равно 600 секундам, что равно 10 минутам.

Время ожидания авторизации

На этот раз управляет периодом времени, Кабельный модем будет ждать ответа от CMTS Cisco при согласовании о KEK впервые.

Можно настроить на этот раз в файле конфигурации DOCSIS путем изменения поля **Authorize Wait Timeout** под вкладкой Baseline Privacy.

Значение по умолчанию для этого поля 10 секунд, допустимый диапазон – от 2 до 30 секунд.

Время ожидания повторной авторизации

На этот раз управляет периодом времени, Кабельный модем будет ждать ответа от CMTS Cisco при согласовании о новом KEK, потому что время жизни KEK собирается истечь.

Это время можно настроить в файле конфигурации DOCSIS, изменив поле Reauthorize Wait Timeout на вкладке Baseline Privacy.

Значение по умолчанию для этого таймера составляет 10 секунд, и допустимый диапазон составляет 2 - 30 секунд.

Время ожидания повторной авторизации

Определяет период отсрочки для повторной авторизации (в секундах). Значение по умолчанию 600. Допустимый диапазон составляет 1 - 1800 секунд.

Время ожидания авторизации отказа

Если Кабельный модем пытается выполнить согласование о KEK с CMTS Cisco, но отклонен, он должен ждать Авторизовать Времени ожидания Отклонения прежде, чем повторно попытаться выполнить согласование о новом KEK.

Можно настроить этот параметр в файле конфигурации DOCSIS при помощи поля **Authorize Reject Wait Timeout** под вкладкой Baseline Privacy. Значение по умолчанию для этого таймера равно 60 секундам, и допустимые значения находятся в интервале от 10 до 600 секунд.

Время ожидания операции

На этот раз управляет периодом времени, Кабельный модем будет ждать ответа от CMTS Cisco при согласовании о TEK впервые.

Это время можно задать в конфигурационном файле DOCSIS посредством изменения в поле Время ожидания операции на вкладке базовой конфигурации конфиденциальности.

Значение по умолчанию для этого поля равно 1 секунде, а диапазон доступных значений составляет от 1 до 10 секунд.

Время ожидания нового ключа

На этот раз управляет периодом времени, Кабельный модем будет ждать ответа от CMTS Cisco при согласовании о новом TEK, потому что срок действия TEK собирается истечь.

Это время можно задать в конфигурационном файле DOCSIS, изменив поле Rekey Wait Timeout на вкладке Baseline Privacy.

Значение по умолчанию для этого таймера составляет 1 секунду, а допустимый интервал

составляет от 1 до 10 секунд.

Команды конфигурации системы базовой конфиденциальности Cisco CMTS Baseline Privacy

Следующие команды кабельного интерфейса могут использоваться для настройки базовой конфиденциальности и зависимые от нее функции на Cisco CMTS.

cable privacy

Команда cable privacy обеспечивает согласование базовой конфиденциальности для конкретного интерфейса. Если **команда no cable privacy** будет настроена на кабельном сопряжении, то никаким кабельным модемам не позволят выполнить согласование о Базовой конфиденциальности, подключаясь к сети на том интерфейсе. Проявите осмотрительность при отключении Базовой конфиденциальности, потому что, если кабельным модемом дают команду использовать Базовую конфиденциальность ее файлом конфигурации DOCSIS, и CMTS Cisco отказывается позволять ему выполнить согласование о базовой конфиденциальности, тогда модем может не быть в состоянии остаться онлайновым.

cable privacy mandatory

Если **команда cable privacy mandatory** настроена, и кабельному модему включили базовую конфиденциальность в ее файле конфигурации DOCSIS, то кабельный модем должен успешно выполнить согласование и использовать Базовую конфиденциальность иначе, не будет позволено остаться онлайновым.

Если файл конфигурации DOCSIS кабельного модема не даст модему команду использовать базовую конфиденциальность тогда**, то команда cable privacy mandatory** не будет мешать модему остаться онлайновой.

Команда cable privacy mandatory не включена по умолчанию.

cable privacy authenticate-modem

Можно заполнить форму проверки подлинности для модемов, задействованных в базовом интерфейсе обеспечения конфиденциальности. Когда кабельные модемы выполняют согласование о KEK с CMTS Cisco, модемы передают подробные данные своего 6-байтового MAC-адреса и своего серийного номера к CMTS Cisco. Эти параметры могут использоваться в качестве сочетания имени пользователя и пароля в целях аутентификации кабельных модемов. Для этого Cisco CMTS использует службу аутентификации, авторизации и учета (AAA) Cisco IOS. Кабельные модемы с ошибками аутентификации не позволяют работать в оперативном режиме. Кроме того, эта команда не касается кабельных модемов, которые не используют базовую секретность.

Внимание. : Так как эта функция использует сервис AAA, необходимо удостовериться, что вы осторожны при изменении конфигурации AAA, иначе можно непреднамеренно потерять способность войти и управлять CMTS Cisco.

Ниже приведено несколько примеров конфигураций для различных способов выполнения

модемной аутентификации. В этих примерах конфигурации в базу данных аутентификации вводится количество модемов. Шестиоктетный MAC-адрес модема служит именем пользователя, а серийный номер переменной длины - паролем. Обратите внимание на то, что один модем был настроен с очевидно неправильным серийным номером.

Следующий частичный образец конфигурации Cisco CMTS использует базу данных локальной проверки подлинности для аутентификации многих кабельных модемов.

```
aaa new-model

aaa authentication login cmts local

aaa authentication login default line

!

username 009096073831 password 0 009096073831

username 0050734eb419 password 0 FAA0317Q06Q

username 000196594447 password 0 **BAD NUMBER**

username 002040015370 password 0 03410390200001835252

!

interface Cable 3/0

 cable privacy authenticate-modem

!

line vty 0 4

 password cisco
```

Другой метод аутентифицирующихся модемов должен был бы использовать внешний сервер RADIUS. Вот частичный пример конфигурации CMTS Cisco, который использует внешний сервер RADIUS для аутентификации модемов

```
aaa new-model

aaa authentication login default line

aaa authentication login cmts group radius

!

interface Cable 3/0

 cable privacy authenticate-modem

!

radius-server host 172.17.110.132 key cisco

!

line vty 0 4

 password cisco
```

Ниже типовой файл базы данных Пользователей RADIUS с аналогичными сведениями к

приведенному выше примеру, который использовал локальную проверку подлинности. Пользовательский файл используется многой рекламой и бесплатными серверами RADIUS как база данных, где хранится информация проверки подлинности пользователя.

```
# Sample RADIUS server users file.


# Joe Blogg's Cable Modem

009096073831 Password = "009096073831"

             Service-Type = Framed


# Jane Smith's Cable Modem


0050734EB419 Password = "FAA0317Q06Q"


             Service-Type = Framed


# John Brown's Cable Modem

000196594477 Password = "**BAD NUMBER**"

             Service-Type = Framed


# Jim Black's Cable Modem

002040015370 Password = "03410390200001835252"


             Service-Type = Framed
```

Показанный ниже выходные данные **команды show cable modem**, выполняемой на CMTS Cisco, который использует любой из вышеупомянутых примеров конфигурации. **После этого все модемы с включенным базовым интерфейсом обеспечения конфиденциальности, не перечисленные в списке локальной базы данных аутентификации или имеющие неверный серийный номер, перейдут в состояние отклонения (pk) и отключатся от сети.**

```
CMTS# show cable modem
Interface   Prim Online      Timing Rec    QoS CPE IP address      MAC address
            Sid  State       Offset Power
Cable3/0/U0 17   online      2810    0.00  6   0   10.1.1.11       0001.9659.43fd
Cable3/0/U1 18   online(pt)  2739    0.00  5   0   10.1.1.29       0050.734e.b419
Cable3/0/U0 19   offline     2815    0.00  2   0   10.1.1.52       0001.9659.4461
Cable3/0/U0 20   reject(pk)  2810   -0.75  5   0   10.1.1.30       0001.9659.4447
Cable3/0/U1 21   online(pt)  2212    0.75  7   0   10.1.1.40       0020.4001.5370
Cable3/0/U0 22   online(pt)  2806    0.00  5   0   10.1.1.44       0090.9607.3831
```

Модем с SID 17 не имеет записи в базе данных проверки подлинности, но в состоянии подключиться к сети, потому что ее файл конфигурации DOCSIS не дал команду, чтобы он

использовал Базовую конфиденциальность.

Модемы с SID, равными 18, 21 и 22, могут перейти в оперативный режим, поскольку им соответствуют правильные записи в базе данных аутентификации

Модем с SID 19 не может подключиться к сети, так как ему была отдана команда использовать базовую секретность, но в базе данных проверки подлинности этого модема нет записи. Этот модем недавно находился в состоянии reject(pk), показывающем, что ему не удалось выполнить аутентификацию.

Модем с SID 20 неспособен подключиться к сети потому что, невзирая на то, что существует запись в базе данных проверки подлинности с MAC-адресом этого модема, соответствующий серийный номер является неправильным. В настоящее время этот модем находится в отклонении (pk) состояние, но перейдет к автономному состоянию после короткого периода.

Когда модемы отказывают аутентификацию, сообщение вдоль следующих линий добавлено к журналу CMTS Cisco.

```
%UBR7200-5-UNAUTHSIDTIMEOUT: CMTS deleted BPI unauthorized Cable Modem 0001.9659.4461
```

Кабельный модем затем удаляется из списка обслуживания станции и обозначается как отключенный через 30 секунд. Кабельный модем затем скорее всего попытается снова подключиться к сети и снова получит отказ.

Примечание: Cisco не рекомендует пользователям использовать команду cable privacy authenticate-modem для запрета установления соединений неуполномоченными кабельными модемами. Более эффективный способ гарантировать, что неавторизованный клиенты не получают доступ к сети поставщика услуг, состоит в том, чтобы настроить систему инициализации, таким образом, что неавторизованные кабельные модемы проинструктированы для загрузки файла конфигурации DOCSIS полевым набором доступа к сети к прочь. В этом случае модем не будет терять ценную пропускную способность восходящего канала из-за постоянного повторного определения диапазона. Вместо этого модем получит к **онлайновому (d)** состояние, которое указывает, что пользователи позади модема не будут предоставленным доступом к сети поставщика услуг, и модем будет только использовать пропускную способность восходящего канала для обслуживания станции.

Команды, используемые для мониторинга состояния BPI

show interface cable X/0 privacy [kek | tek] — Эта команда используется для отображения таймеров, привязанных или к KEK или к TEK, как установлено на интерфейсе CMTS.

Ниже пример выходных данных этой команды.

```
CMTS# show interface cable 4/0 privacy kek Configured KEK lifetime value = 604800 Configured KEK
grace time value = 600 CMTS# show interface cable 4/0 privacy tek Configured TEK lifetime value
= 60480 Configured TEK grace time value = 600
```

show interface cable X/0 privacy statistic — Эта команда hidden может использоваться для просмотра статистики по количеству SID с помощью базовой конфиденциальности на интерфейсе определенного кабеля.

Ниже пример выходных данных этой команды.

```
CMTS# show interface cable 4/0 privacy statistic CM key Chain Count : 12 CM Unicast key Chain
Count : 12 CM Mucast key Chain Count : 3
```

debug cable privacy — Эта команда активирует отладку Базовой конфиденциальности. Когда эта команда активирована, каждый раз, когда изменение в состоянии Базовой конфиденциальности или событии Базовой конфиденциальности происходит, подробные данные будут отображены на консоли. Эта команда только работает, когда предшествуется с **интерфейсным кабелем debug cable X/0** или *команда mac-address* **mac-address debug cable**.

debug cable bpiatp — Эта команда активирует отладку Базовой конфиденциальности. Когда эта команда активирована, каждый раз, когда сообщение Базовой конфиденциальности передано или получено CMTS Cisco, шестнадцатеричный дамп сообщения будет отображен. Эта команда только работает, когда предшествуется с **интерфейсным кабелем debug cable X/0** или *команда mac-address* **mac-address debug cable**.

debug cable keyman — Эта команда активировала отладку управления ключами Базовой конфиденциальности. Когда эта команда является активированными подробными данными управления ключами Базовой конфиденциальности, отображены.

Поиск и устранение ошибок в BPI

Кабельные модемы находятся в состоянии online, а не в состоянии online(pt).

Если модем находится в состоянии online, а не в состоянии online(pt), возможны три следующих варианта.

Первой вероятной причиной может быть отсутствие файла конфигурации DOCSIS в кабельном модеме, где указано, что модем использует базовый интерфейс защиты. Проверьте, чтобы в файле конфигурации DOCSIS был выключенный BPI в профиле класса сервиса, посланного модему.

Вторая причина появление модема в оперативном режиме может состоять в том, что модем ожидает завершения согласования BPI. Подождите одну-две минуты и посмотрите, не изменится ли состояние модема на online(pt).

Последняя причина может заключаться в том, что модем не содержит микропрограмму, поддерживающую базовый интерфейс обеспечения конфиденциальности. Свяжитесь со своим поставщиком модема для более свежей версии микропрограмм, которая действительно поддерживает BPI.

Кабельные модемы переходят в состояние reject(pk), а затем в автономный режим.

Наиболее вероятная причина перехода модема в состояние reject(pk) состоит в том, что была настроена аутентификация кабельного модема с помощью команды cable privacy authenticate-modem, но неправильно настроена аутентификация AAA. Проверьте, чтобы все серийные номера и MAC-адреса используемых модемов были правильно введены в базу данных проверки подлинности и что все внешние сервера RADIUS доступны и находятся в рабочем состоянии. **Можно использовать команды отладки маршрутизатора debug aaa authentication и debug radius для получения представления о состоянии сервера RADIUS или о причине ошибки аутентификации модема.**

Примечание: Для получения общей информации об устранении проблем подключения

через кабельный модем обратитесь к Устранению проблем Кабельных модемов uBR, Не Подключающихся к сети.

Специальное примечание - скрытые команды

Любое упоминание о скрытых командах в данном документе используется только с целью ознакомления. Команды hidden не поддерживаются Центром технической поддержки Cisco (TAC). Кроме того, команды hidden:

- Не всегда создает надежные или правильные сведения
- Может иметь неожиданные побочные эффекты
- Может не вести себя тот же путь в других версиях программного обеспечения Cisco IOS
- Может быть удален из будущих версий программного обеспечения Cisco IOS в любое время без предупреждения

Дополнительные сведения

- CableLabs
- Конфигуратор клиентского оборудования DOCSIS
- Аутентификация, авторизация и учет (AAA)
- Техническая поддержка - Cisco Systems